

REMARKS

In the Office Action, the Examiner rejected the claims under 35 USC §102 and 35 USC §103. The claims have been amended to further clarify the subject matter regarded as the invention. The rejections are fully traversed below. New claim 55 has been added. Claims 1-4, 6-31, and 33-55 are now pending.

Reconsideration of the application is respectfully requested based on the following remarks.

REJECTION OF CLAIMS UNDER 35 USC §102

In the Office Action, the Examiner has rejected claims 1-10, 13-36, and 38-53 under 35 USC §102(e) as being anticipated by Yokote, U.S. Patent Pub. No. 2002/0147820, ('Yokote' hereinafter). This rejection is fully traversed below.

Claim 1, as amended, is directed to a method performed by a server. Claim 1 recites, in part:

deriving key information from a key or password associated with the Mobile Node;
and

sending a reply message to the Home Agent, the reply message including the key information associated with the Mobile Node, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information;

wherein the reply message does not include the shared key to be shared between the Mobile Node and the Home Agent in any form.

Yokote discloses a method for implementing IP security in Mobile IP networks. See title. More particularly, a sending node initiates the establishment of a security association

for a receiving node. See Abstract. For instance, as shown in FIGs. 6 and 7 of Yokote, a Correspondent Node (CN) initiates the establishment of a security association for a Mobile Node by contacting a Ticket Granting Server (TGS). It is also important to note that once the TGS generates a session key, the TGS transmits the session key to the CN, which then transmits the session key to the Mobile Node. In other words, the Mobile Node does not need to generate or otherwise derive the session key.

In the Final Office Action mailed August 20, 2007, the Examiner states that “Yokote teaches, at figure 6, that an authentication request is made by a first entity. A response is sent back from a second entity that includes a ticket and session key, both encrypted using a secret key of the first entity. At this point, the first entity uses its secret key to decrypt the encrypted ticket and session key. It is only after the decryption step that the session key can be used by the two entities.” The Examiner further asserts that “the reply message, sent from the second entity to the first entity, does not include the shared key, but rather encrypted data that is unintelligible by the entities until a proper decryption takes place.” Applicant respectfully traverses this assertion.

Although the Examiner asserts that the reply message includes encrypted data that is unintelligible until decrypted, Applicant respectfully asserts that the data that the Examiner refers to includes the session key. In other words, the reply transmits the shared key, which has been encrypted. Although it cannot be used until it is decrypted, the reply message of Yokote does, in fact, include the session key.

In contrast, the claimed invention does not transmit a session key in any form (encrypted or otherwise). Rather, the entity communicating with the server separately derives the session key. For instance, as recited in claim 1, a server may derive key information (not the final key) and send the key information to the Home Agent in a registration reply, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information. The Home Agent may then derive a key to be shared between the Mobile Node and the Home Agent from the key information.

In order to clarify the subject matter being claimed, Applicant has amended claim 1 to clarify that the reply message does not include the shared key in any form. As recited in newly added claim 55, the reply message does not include the shared key in encrypted form or decrypted form. Thus, the shared key cannot be retrieved from the reply message of claim 1, either with or without decryption.

Claim 10, as amended, is directed to a method performed by a Home Agent. Claim 10 recites, in part:

deriving a key from the key information, the key being a shared key between the Mobile Node and the Home Agent, wherein deriving the key from the key information does not include decryption of the key information; and

sending a Mobile IP registration reply to the Mobile Node, wherein the Mobile IP registration reply does not include the key in any form

As recited in claim 10, the Home Agent derives the key, where the key is a shared key between the Mobile Node and the Home Agent. It is important to note that deriving the key from the key information does not include decryption of the key information. In addition, the Home Agent does not transmit the key to the Mobile Node in any form (encrypted or otherwise). Rather, the Mobile IP registration reply that is sent to the Mobile Node does not include the key. Therefore, the Mobile Node must separately derive the key.

For example, claim 36 is directed to a method performed by a Mobile Node. Claim 36 recites, in part:

receiving a registration reply from the Home Agent, the registration reply indicating that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent, wherein the registration reply does not include the key to be shared between the Mobile Node and the Home Agent in any form; and

deriving a key to be shared between the Mobile Node and the Home Agent from key information stored at the Mobile Node, wherein deriving the key from the key information does not include decryption of the key information.

It is clear from claim 36 that the Mobile Node derives the key to be shared between the Mobile Node and the Home Agent. It is important to note that the registration reply does not include the key in any form (encrypted or otherwise). Deriving the key from the key information does not include decryption of the key information. In addition, the registration reply indicates that the Mobile Node is to derive the key. The cited art fails to disclose or suggest that the Mobile Node must independently derive the key, or that the registration reply

indicates that the Mobile Node is to derive the key.

A rogue node could conceivably determine the secret key in Yokote and use the secret key to decrypt the session key. As a result, communications transmitted between the Mobile Node and the Home Agent and encrypted using the session key would thereafter be insecure. In contrast, with respect to the invention of claim 1, even if a rogue node could obtain the key information transmitted by a server to the Home Agent, communications between the Mobile Node and the Home Agent would continue to be secure, since the rogue node would not be in possession of the session key in either encrypted or non-encrypted form. As a result, the pending claims provide a more secure mechanism for generating session keys than the cited art.

As set forth above, Yokote transmits a session key that is encrypted, and therefore needs to be decrypted. In contrast, the claimed invention requires that the session key be independently derived by the Home Agent and the Mobile Node.

The remaining independent claims are patentable for similar reasons. The dependent claims depend from one of the independent claims and are therefore patentable for at least the same reasons. However, the dependent claims recite additional limitations that further distinguish them from Yokote.

For example, with respect to claim 15, the Examiner asserts that Yokote teaches “wherein the Mobile Node is to derive the shared key from a second set of key information stored at the Mobile Node,” citing paragraph 0061. However, Applicant was unable to find any reference to a Mobile Node in this paragraph. Therefore, Yokote fails to disclose or suggest a Mobile Node deriving a shared key from a second set of key information stored at the Mobile Node. In fact, Applicant respectfully asserts that Yokote fails to disclose or suggest a Mobile Node deriving a shared key in any manner. Applicant therefore respectfully submits that claim 15 is patentable over Yokote.

Moreover, with respect to claim 21, the Examiner asserts that Yokote teaches that the registration reply indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent, citing Fig. 6, ref. num. S6-3. However, ref. num. S6-3 actually illustrates a TGS creating a session key in order to transmit the session key to a Correspondent Node. In fact, ref. num. S6-3 fails to disclose or suggest sending a registration reply in any manner. Moreover, S6-3 fails to show a Mobile Node. Accordingly, Applicant respectfully submits that claim 21 is patentable over Yokote.

As yet another example, claim 31 recites that “the key information is derived from a

password associated with the Mobile Node.” Although Yokote discloses that a user enters a username, Applicant respectfully asserts that Yokote fails to disclose or suggest deriving key information from the username, enabling a shared key between a Mobile Node and a Home Agent to be derived from the key information. Accordingly, Applicant respectfully submits that Yokote fails to anticipate claim 31.

The additional limitations recited in the independent claims or the dependent claims are not further discussed, as the above discussed limitations are clearly sufficient to distinguish the claimed invention from the cited reference. Thus, it is respectfully requested that the Examiner withdraw the rejection of the claims under 35 USC §102.

REJECTION OF CLAIMS UNDER 35 USC §103

In the Office Action, the Examiner has rejected claims 11, 12, and 37 under 35 USC §103(A) as being unpatentable over Yokote in view of Abrol et al, U.S. Patent. No. 6,785,823, (‘Abrol’ hereinafter). This rejection is fully traversed below.

As set forth above, Yokote teaches the transmission of a session key. As such, Yokote teaches away from the claimed invention, which does not transmit a session key between entities in any form. As such, Yokote teaches away from the independent derivation of the session key by entities such as the Home Agent and Mobile Node, as recited in claims 1 and 10, respectively.

The Examiner further cites Abrol. However, Abrol fails to cure the deficiencies of Yokote. It is also important to note that although Abrol does disclose a CHAP Challenge and a CHAP Response, Abrol fails to disclose or suggest a registration request that includes a CHAP Challenge or CHAP Response. In fact, FIG. 2, cited by the Examiner, shows that a Mobile IP registration request is transmitted separately from the CHAP Challenge and CHAP Response. More particularly, the Mobile IP registration request of Abrol is transmitted after the CHAP Challenge/Response messages are transmitted. As a result, the combination of the cited references would fail to achieve the desired result. It is also important to note that the cited references, separately or in combination, fail to disclose or suggest deriving a key from

information in a CHAP Challenge or CHAP response. Accordingly, the combination of the cited references would fail to operate as claimed.

The cited references, separately or in combination, fail to disclose or suggest the disadvantages of transmitting a session key between entities. Moreover, the cited references fail to disclose or suggest a solution to such a problem. Accordingly, Applicant respectfully submits that 11, 12, and 37 are patentable over the cited references.

SUMMARY

If there are any issues remaining which the Examiner believes could be resolved through either a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned attorney at the telephone number listed below.

Applicants hereby petition for an extension of time which may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 50-0388 (Order No. CISCP334).

Respectfully submitted,
BEYER WEAVER LLP

/Elise R. Heilbrunn/
Elise R. Heilbrunn
Reg. No. 42,649

P.O. Box 70250
Oakland, CA 94612-0250
Tel: (510) 663-1100